Securing Your Tomorrow®

Time for Universities to Teach Cybercriminals a Lesson

SIX KEYS TO SECURE PEACE OF MIND FOR STUDENTS, FACULTY, AND STAFF

Learning the Hard Way

Thanks to cybercriminal intrusions that cost billions and disrupted university services and functioning, the higher education sector has learned the hard way about cybersecurity. However, the security techniques and technology that other sectors have deployed can be quickly adapted for university systems – and none too soon. For example, in Australia, the government prepares to enforce an "enhanced framework to uplift security and resilience" upon universities. Moreover, students, faculty, researchers, and IT professionals everywhere are increasingly sensitive to a university's cybersecurity performance and making cybersecurity strength a firm competitive advantage.

Unsurprisingly, the COVID-19 pandemic exposed the higher education sector's susceptibility to cybersecurity attacks. While the rush to virtual learning may have allowed for a massive increase in attacks, the truth is, cybercriminals have long been aware that higher education is a target-rich, insufficiently defended environment.

According to Comparitech, in July and August 2020, while all industries experienced a 6.5% increase in cybersecurity attacks, the increase was an alarming 30% for higher educational institutions.

A Sizeable and Urgent Challenge

According to the FBI, online crimes reported to the Bureau's Internet Crime Complaint Center (IC3) have increased by 400% due to the pandemic, with as many as 4,000 incidents per day.

FBI's Cyber Division warned in early March 2021 that criminals using malicious ransomware software are steadily targeting more education institutions and attempting to extort them.

And ransoms extracted are costly – almost half a million dollars in the case of the University of Utah, for example – to say nothing of the reputational cost. Even if there is no data lost, system downtime when responding to a suspected breach can vastly disrupt a university's ability to deliver its services.

Information like educational records is one of the most sought-after data for cybercriminals and can fetch up to $265 on the black market.

Since 2016, cybersecurity attacks targeting the education sector have increased by fivefold. The switch to virtual learning environments due to the coronavirus pandemic has increased opportunities for hackers. In July 2021, the sector saw a 29% increase in attacks compared to July 2020.

A Favorite Target

There is good reason for higher education's appeal to intruders: There are vast stores of valuable information about students, staff, vendors, and alumni that intruders can monetize, and vital research data can be sold to shady nation states. A security talent shortage leaves higher education competing at a disadvantage with the private sector. The decentralized structure of the academic world enables disparate departments to invest in their own IT without the oversight of security professionals – creating shadow IT. Universities have a culture of sharing information within the university and other schools, governments, and private entities.

And finally, university networks serve many different types of individuals with various devices who expect ready access to a vast number of systems across numerous locations, offering intruders multiple entry points to compromise. The University of Northampton fell prey to a cyberattack, which led to the disruption of its telephone and IT systems and servers. The University of California, San Francisco paid a ransom of $1.14 million after the NetWalker ransomware locked down multiple servers of its School of Medicine in June 2020. Monitoring and responding to these environments is a tricky business.

Results from the 2021 Unisys Security Index™ for the United States indicate heightened recognition of cyber vulnerabilities and growing concern. The findings pose a stark warning for companies navigating remote and hybrid work environments, trying to balance productivity and security.

Six Keys for Better Security

With so many vulnerabilities, how can the sector provide the level of cybersecurity its constituents deserve and expect? By adopting a variety of measures proven in other sectors.

1. **Limit damage** - You are bound to have many legacy systems, and they are likely to have vulnerabilities – accept that as a fact, patch them as best you can, and accept that you will experience a breach accordingly. Your responsibility is to ensure that the inevitable breach doesn't lead to a wholesale penetration of your environment, meaning lateral movement of the intruder across your network, which is how serious damage occurs. By micro-segmenting your systems, you can wall off intruders from your most sensitive information.

2. **Test your defenses** - Don't let criminals be your cybersecurity quality control. Don't wait to be attacked to see if your defenses work. Do your own penetration testing. Test, test, test. Exploit your own vulnerabilities and prevent ransomware and exfiltration of data not only to be in compliance but to demonstrate a strong security posture. This includes testing people to see if they will fall for a dummy attack. Especially if they accept payment cards, as universities do, you are obliged to comply with the Payment Card Industry Data Security Standard (PCI DSS) with penetration testing every six months.

3. **Verify, don't trust** - In today's hyper-security environment, there's no alternative to adopting the concept of Zero Trust. That means exactly what it says. Nobody knocking at your network door is to be trusted to be who they say they are. Every person or device seeking access must be able to verify any and everything before being granted access. Zero Trust is a posture, principles, and architecture. It is a journey of many steps: authenticating users and allowing least-privilege access. Micro-segmenting mission-critical systems. Asset discovery and inventory management. And so on. Start now with your top priorities – your most sensitive data and systems – and build security into them.

4. **A holistic security mindset** - There is also a critical cultural aspect to cybersecurity. It requires a holistic mindset that unites all parts of the university in thinking about security in everything they do, rather than siloed departments making their own decisions, purchases, policies, and procedures. All parties must focus as much on security as on availability, access, and capacity – and all driven from the top. Cybersecurity belongs in every conversation at the top of the organization. Your cybersecurity leaders and partners belong in every strategic conversation.

5. **Internal accountability** - It can be tempting to simply outsource security responsibilities to vendors with impressive credentials, but that is a dangerous mistake. No outside party can be as familiar with your organization, its strategies, its systems, its day-to-day operations, and its people, as well as internal experts whose entire focus is on your university. To be sure, they will want reliable partners with extensive experience who can advise them on best practices and common mistakes. But ultimately, if you suffer a breach, it will be your university, not the vendor, in the damning headlines, so keep it within your authority.

6. **Education is forever** - Educate your users – and re-educate them every time a new lesson is learned from another entity's misfortune. Cybercriminals are often highly sophisticated operators who have all the time in the world to probe your defenses, trick your users, and deploy innovative schemes. Make sure your users know how these tricks work, how damaging they can be, and how to avoid and report them. Don't settle for memos and alerts that might not be noticed. Require affirmative acknowledgement and proof of compliance. And don't forget – learning embeds best when it is engaging. Don't make people feel guilty – and don't be afraid to make it fun.

The good news is that the pandemic escalated the transition to digital education and highlighted the critical importance of a university's IT systems. But it also exposed its unique vulnerabilities. Cybersecurity is now an urgent priority and a competitive advantage for higher education. The path is clear for university leaders and their cyber experts to earn the security credentials that their constituents need and expect.

To learn more about how Unisys cloud solutions and services can help your university become cyber-resilient, contact us.

For more information visit www.unisys.com